



GUIDE

# 12 Critical Threat Modeling Gaps in Medical Device Submissions

*A practical, ungated guide to the threat modeling gaps that trigger FDA cybersecurity questions in 510(k), De Novo, and PMA submissions - and exactly how to close them before reviewers find them.*

Threat Modeling • Medical Devices • FDA Premarket

A practical, ungated guide to the threat modeling gaps that trigger FDA cybersecurity questions, and exactly how to close them before reviewers find them.

## Why Threat Modeling Is Now a Gating Activity, Not a Checkbox

FDA 2026 Premarket Cybersecurity Guidance (aligned to Section 524B of the FD&C Act) emphasizes secure product development, system threat modeling, security risk management, architecture views, SBOM traceability, and testing evidence. Reviewers need to understand how your device and related systems are cybersecure across the total product lifecycle.

The patterns repeat. Across connected medical device submissions, the same threat modeling gaps appear again and again: incomplete system boundaries, weak assumptions, missing safety-risk traceability, and controls that are not tied to verification evidence.

Use this guide to pressure-test your threat model before pre-submission, 510(k), De Novo, PMA, or IDE documentation is finalized.

## How to Use This Guide

Read each gap as a self-assessment against your current architecture package. Use the fix list to assign owners across engineering, quality, regulatory, and security. Where a gap exists, update both diagrams and explanatory text so the reviewer can follow the risk story.

- Engineering Teams
- Quality & Regulatory
- Security Reviewers
- Submission Writers



## **| The 12 Most Common Critical Gaps**

Use each gap as a checklist item against your current architecture package before finalizing any FDA premarket submission.

### **1. Missing Global System View**

**What We See in Submissions:** The submission describes the device, but not the device plus cloud, mobile app, hospital network, update server, service tools, users, and external dependencies.

**How to Fix It:** Create a full medical device system diagram with assets, interfaces, trust boundaries, data flows, user roles, and environment-of-use assumptions.

### **2. No Hostile-Network Assumption**

**What We See in Submissions:** Threats are scoped as if hospital or home networks are trusted, even though FDA recommends assuming adversaries can alter, drop, and replay traffic.

**How to Fix It:** Document hostile network assumptions and map controls for authenticity, authorization, confidentiality, availability, and replay protection.

### **3. Safety Risk and Security Risk Are Disconnected**

**What We See in Submissions:** The threat model lists cyber threats but does not show how exploitation could cause patient harm, delayed care, incorrect diagnosis, or therapy disruption.

**How to Fix It:** Trace each credible threat to clinical function, safety impact, risk controls, residual risk, and safety-risk-management outputs - per ISO 14971.

### **4. Update Path Is Under-Modeled**

**What We See in Submissions:** Patchability is described at a high level, but the end-to-end update chain, signatures, rollback protection, and deployment failure modes are not analyzed.

**How to Fix It:** Build an updateability and patchability view covering servers, delivery paths, device validation, rollback, logging, and lifecycle support.

### **5. Multi-Patient Harm Is Ignored**

**What We See in Submissions:** Connected devices can fail or be compromised at scale, but the model only evaluates one device and one patient at a time.

**How to Fix It:** Add multi-patient harm scenarios for shared infrastructure, cloud outages, fleet commands, common credentials, and simultaneous compromise.

### **6. SBOM Risks Are Not Linked**

**What We See in Submissions:** The SBOM exists, but third-party components, end-of-life libraries, supplier constraints, and known vulnerabilities are not connected to the threat model.

**How to Fix It:** Tie SBOM components to threat scenarios, vulnerability monitoring, compensating controls,



[support plans, and risk acceptance rationale.](#)

## **7. Security Use Cases Are Too Generic**

**What We See in Submissions:** The model says data is sent or received, but does not assess clinical states like programming, alarming, standby, diagnostics, therapy delivery, or maintenance.

**How to Fix It:** Create security use-case views for the device functions where compromise could affect safety or effectiveness.

## **8. Residual Risk Rationale Is Thin**

**What We See in Submissions:** Controls are listed, but the submission does not explain pre- and post-mitigation risk, exploitability, assumptions, or why residual risk is acceptable.

**How to Fix It:** Use a consistent security risk scoring method and provide traceability from threat to control, testing evidence, and residual risk conclusion.

## **9. Manufacturing and Service Workflows Are Omitted**

**What We See in Submissions:** Provisioning, service access, calibration tools, debug ports, maintenance laptops, and decommissioning are excluded from the model.

**How to Fix It:** Model manufacturing, deployment, maintenance, service, and decommissioning workflows as part of total product lifecycle cybersecurity - tied to your SPDF documentation.

## **10. Testing Does Not Map Back to Threats**

**What We See in Submissions:** Penetration testing and verification reports exist, but reviewers cannot see which threat-model controls were actually tested.

**How to Fix It:** Create a traceability matrix linking threats, controls, security requirements, test evidence, unresolved anomalies, and risk decisions. See our pen test findings guide.

## **11. Assumptions Are Undocumented**

**What We See in Submissions:** The model depends on hospital firewalling, user behavior, network segmentation, or supplier updates, but those assumptions are not stated or justified.

**How to Fix It:** State assumptions explicitly and identify which risks are transferred to users, operators, healthcare facilities, suppliers, or labeling - per AAMI TIR57.

## **12. Reviewer Narrative Is Missing**

**What We See in Submissions:** The technical artifacts may be accurate, but the submission does not tell a clear FDA-facing story about secure design and safety effectiveness.

**How to Fix It:** Add concise explanatory text that connects SPDF, architecture views, threat modeling, SBOM, testing, and risk management into one evidence story. See common FDA rejection reasons.



**Ready to talk through your roadmap?**

**[Book a Strategy Session →](#)**

*Source guide: 12-critical-threat-modeling-gaps-medical-device-submissions. For the most current version, visit [bluegoatcyber.com/guides/12-critical-threat-modeling-gaps-medical-device-submissions](https://bluegoatcyber.com/guides/12-critical-threat-modeling-gaps-medical-device-submissions).*